

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВПО «ВОЛОГОДСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ
УНИВЕРСИТЕТ»
ФИЗИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

УТВЕРЖДАЮ



06 сентября 2011г.

Рабочая программа дисциплины (модуля)

ТЕОРИЯ ЧИСЕЛ

Специальность
050201 «Математика»

Форма обучения
ЗАОЧНАЯ

Вологда
2011

Рецензент (ы) проф., д.ф.-м.н. Губа В.С.

протокол № 1 от 06 сентября 2011 года.

[illegible]

1. Цели освоения дисциплины

Целью освоения дисциплины является понимание отношения делимости и сравнимости по модулю для целых чисел, понятие простого числа.

2. Место дисциплины в общей системе подготовки специалиста

Цикл ДПП.

3. Требования к уровню освоения содержания дисциплины

В результате изучения курса студент должен *иметь представление*:

- о месте и роли теории чисел в системе математических наук;
- об основных приложениях теории чисел как внутри математики, так и в других областях, в частности в защите информации.

Студент должен *знать*:

- основы теории делимости в кольце целых чисел;
- основные арифметические функции;
- теорию числовых сравнений;
- теорию сравнений с неизвестными;
- теорию первообразных корней и методы решения задачи дискретного логарифмирования;
- теорию цепных дробей и их применение в решении задач, в частности, в приближениях;
- понятия алгебраических и трансцендентных чисел.

Студент должен *уметь*:

- находить НОД и НОК целых чисел;
- решать в целых числах линейные уравнения и их системы;
- отделять простые числа в заданном диапазоне;
- осуществлять факторизацию числа;
- использовать арифметические функции их свойства в решении задач;
- представлять рациональные числа бесконечными десятичными дробями;
- проверять числа на простоту;
- решать сравнения первой степени с одним неизвестным;
- решать системы сравнений первой степени с одним неизвестным;
- решать полиномиальные сравнения по простому и составному модулям;
- вычислять значения символа Лежандра и символа Якоби;
- строить первообразные корни по заданным модулям;
- строить цепные дроби и использовать их в решении задач.

Таким образом, студент должен научиться использовать методы теории чисел для решения теоретических и прикладных задач.

4. Извлечение из ГОС ВПО специальности (162 ЧАСА)

Делимость и простые числа. Основная теорема арифметики. Основное свойство простого числа. Неравенства Чебышева для $\pi(x)$. Теория сравнений. Кольцо и поле классов вычетов. Теоремы Эйлера и Ферма. Сравнения и системы сравнений с неизвестной величиной. Сравнения первой степени. Сравнения по простому модулю. Сравнения по степени простого числа. Редукция сравнения по составному модулю к сравнению по степени простого числа и к сравнению по простому модулю. Показатели чисел и классов по данному модулю. Число классов с заданным показателем. Теорема о существовании первообразного корня по простому модулю. Индексы чисел и классов по данному модулю. Двучленные сравнения по простому модулю. Квадратичные вычеты и невычеты. Символ Лежандра. Арифметические приложения теории сравнений. Цепные дроби. Существование и единственность значения цепной дроби. Представление

действительных чисел цепными дробями. Теорема Лагранжа о квадратичной иррациональности. Приближения действительных чисел подходящими дробями. Теорема Дирихле и ее применение к представлению простого числа $p \equiv 1 \pmod{4}$ в виде суммы двух квадратов. Алгебраические и трансцендентные числа. Теорема Лиувилля и ее применение к построению трансцендентных чисел и к доказательству иррациональности.

5. Структура и содержание дисциплины «Теория чисел»

5.1 Общая трудоемкость дисциплины составляет 162 час.

№ п/п	Название темы	Лекции (час)	Практические занятия
1	Разложение чисел на простые множители	1	1
2	Распределение простых чисел (обзор)	1	
3	Теоретико-числовые функции	1	1
4	Сравнения и системы сравнений с неизвестной	1	1
5	Конечные цепные дроби	1	1
6	Диофантовы уравнения	1	1
7	Порядок числа и класса вычетов	1	1
8	Первообразные корни	1	1
9	Индексы чисел и классов вычетов	1	1
10	Квадратичные вычеты и невычеты	1	1
	Арифметические приложения теории сравнений	1	1
	Бесконечные цепные дроби		1
	Алгебраические и трансцендентные числа		
	Итого (час)	8	8

5.2 Содержание разделов дисциплины.

Отношение делимости в кольце целых чисел.

Простые числа и их основные свойства. Разложение чисел на простые множители. Основная теорема арифметики. Распределение простых чисел (обзор).

Важнейшие теоретико-числовые функции. Функция Эйлера.

Сравнения и их основные свойства. Кольцо и поле классов вычетов.

Теоремы Эйлера, Ферма и Вильсона.

Сравнения и системы сравнений с неизвестной. Конечные цепные дроби. Подходящие дроби и их применение к решению сравнений. Сравнения по простому модулю и по степени простого числа. Редукция сравнения по составному модулю к сравнениям по простому модулю и по степени простого числа.

Порядок числа и класса вычетов по данному модулю. Число классов с заданным порядком. Первообразные корни. Теорема о существовании первообразного корня по простому модулю.

Индексы чисел и классов вычетов по данному модулю. Двучленные сравнения по простому модулю. Квадратичные вычеты и невычеты. Символ Лежандра.

Арифметические приложения теории сравнений. Признаки делимости, определение длины периода десятичной дроби.

Бесконечные цепные дроби. Представление действительных чисел цепными дробями.

Алгебраические и трансцендентные числа.

6. Учебно-методическое обеспечение дисциплины.

Основная

1. Бухштаб А.А. Теория чисел: учебное пособие/ А. А. Бухштаб. – СПб. [и др.]: Лань, 2008.–384 с. 20 экз
2. Виноградов И.М. Основы теории чисел: учебное пособие/ И. М. Виноградов. – СПб. [и др.]: Лань, 2009.–176 с. 5 экз
3. Курош А.Г. Курс высшей алгебры: учеб. для вузов по специальностям "Математика", "Прикладная математика"/ А. Г. Курош. – СПб.; М., Краснодар: Лань: Физматкнига, 2007. –432 с. 20 экз

Дополнительная

1. Айерленд К., Роузен М. Классическое введение в современную теорию чисел. –М.: Мир, 1987.
2. Галочкин А.И., Нестеренко Ю.В., Шидловский А.Б. Введение в теорию чисел. –М. Изд-во МГУ, 1984.
3. Гельфонд А.О. Решение уравнений в целых числах. М.: , 1957.
4. Девенпорт Г. Высшая арифметика. М.: Наука, 1965.
5. Жмулева А.В., Степанова Л.Л. Арифметика. Практикум по решению задач. М.: Изд-во МПГИ, 1986.
6. Калужнин Л.А. Основная теорема арифметики. М.: Наука, 1969.
7. Мальцев Ю.Н. Основная теорема арифметики. // Сб. "Олимпиады, алгебра, комбинаторика". Новосибирск, Наука, 1979.
8. Родосский К.А. Алгоритм Евклида. М.: Наука, 1988.
9. Серпинский В. О решении уравнений в целых числах. М.: Физматгиз, 1961
10. Бухштаб А.А. Теория чисел. -М.: Просвещение, 1966.
11. Виноградов И.М. Основы теории чисел. -М.: Наука, 1981.
12. Грибанов В.У., Титов П.И. Сборник упражнений по теории чисел. -М.: Просвещение, 1964.
13. Кудреватов Г.А. Сборник задач по теории чисел. –М.: Просвещение, 1970.
14. Михелович Ш.Х. Теория чисел. -М.: Высшая школа, 1967.
15. Куликов Л.Я. Алгебра и теория чисел. -М.; Высшая школа, 1979. -559 с.

7. Материально-техническое обеспечение

Освоение дисциплины предполагает использование академической аудитории для проведения лекционных и семинарских занятий, оснащенной необходимыми техническими средствами (компьютер, проектор, экран).

8. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины:

Вопросы для подготовки к зачету

1 Теория делимости. Простые и составные числа

Сформулируйте аксиому индукции.

Докажите, что отношение делимости рефлексивно, симметрично и транзитивно.

Какими еще свойствами обладает отношение делимости?

Сформулируйте теорему о делении с остатком.

Дайте определение НОД двух чисел.

Дайте определение НОК двух чисел.

Как связаны значения НОД и НОК?

Для решения какой задачи предназначен алгоритм Евклида?

Запишите алгоритм Евклида.

Для решения какой задачи предназначен расширенный алгоритм Евклида?

Сформулируйте его.

Сформулируйте обобщенный алгоритм Евклида.
Какое уравнение называется диофантовым?
Как решить линейное диофантово уравнение с двумя неизвестными с помощью РАЕ?

Как решить линейное диофантово уравнение с двумя неизвестными матричным способом?

Как решить систему линейных диофантовых уравнений?

Дайте определение простого числа.

Дайте определение составного числа.

Для решения какой задачи предназначен алгоритм «Решето Эратосфена»?

Сформулируйте алгоритм «Решето Эратосфена».

Конечно или бесконечно множество простых чисел? Обоснуйте свой ответ.

Сформулируйте основную теорему арифметики.

Дайте определение взаимно простых чисел.

Что называется целой частью действительного числа x ?

Что называется дробной частью действительного числа x ?

Запишите неравенства Чебышева.

Какая функция называется дзета-функцией Римана?

2 Арифметические функции

Дайте определение мультипликативной функции.

Перечислите способы построения мультипликативных функций.

Дайте определение функции Мебиуса.

Запишите формулу обращения Мебиуса.

Дайте определение функции Эйлера.

Какие функции выражают сумму делителей и число делителей натурального числа?

Приведите оценки среднего значения арифметических функций.

3 Сравнения и их свойства. Сравнения с одной переменной

Дайте определение чисел, сравнимых по модулю m .

Перечислите свойства отношения сравнимости.

Опишите кольцо классов вычетов по данному модулю.

Когда кольцо классов вычетов по данному модулю образует поле?

Дайте определение полной системы вычетов по заданному модулю.

Дайте определение приведенной системы вычетов по заданному модулю.

Сформулируйте теорему Вильсона.

Сформулируйте теорему Эйлера.

Сформулируйте малую теорему Ферма.

Расскажите про представление рациональных чисел бесконечными десятичными дробями.

Каковы вероятностные алгоритмы проверки простоты?

Запишите вид сравнения первой степени. Как его решить?

Сформулируйте греко-китайскую теорему об остатках.

Сформулируйте теорему Лагранжа о решении полиномиальных сравнений по простому модулю.

Каков алгоритм построения множества M делителей многочлена $f(x)$ в кольце $FP[x]$?

Как решить полиномиальное сравнение по составному модулю?

Что называется квадратичным вычетом по модулю p ?

Что называется символом Лежандра? Каковы его свойства?

Сформулируйте квадратичный закон взаимности.

Что называется символом Якоби? Каковы его свойства?

4 Первообразные корни и индексы

Дайте определение первообразного корня по модулю m .

Сформулируйте лемму о свойствах показателей.

Сформулируйте теорему о существовании первообразных корней.

В каком случае возможно построение первообразных корней? Как их построить?

В каком случае отсутствуют первообразные корни?

Что называется индексом числа a по модулю m при основании g ?

Сформулируйте свойства индексов.

Сформулируйте задачу дискретного логарифмирования.

Каков текущий рекорд дискретного логарифмирования?

Как решается задача дискретного логарифмирования?

5 Цепные дроби

Сформулируйте теорему Дирихле о приближении действительных чисел рациональными.

Какая дробь называется цепной?

Как вычислить конечную цепную дробь?

Какие дроби называются подходящими для данной цепной дроби?

Как цепные дроби помогают решать диофантовы уравнения?

Какие еще приложения цепных дробей Вы знаете?

6 Алгебраические и трансцендентные числа

Когда комплексное число называется алгебраическим?

Что такое минимальный многочлен алгебраического числа α ?

Укажите некоторые свойства минимального многочлена.

Что называется трансцендентным числом?

Кем доказано существование трансцендентных чисел?

Приведите примеры трансцендентных чисел.